

File 344:CHINESE PATENTS ABS APR 1985-2001/May

(c) 2001 EUROPEAN PATENT OFFICE

File 347:JAPIO OCT 1976-2001/JAN (UPDATED 010507)

(c) 2001 JPO & JAPIO

File 350:Derwent WPIX 1963-2001/UD,UM &UP=200129

(c) 2001 Derwent Info Ltd

Set Items Description

S1 777911 PROBE? ? OR SENTRY OR SCANNER? ? OR SENSOR? ?

S2 1974041 MONITOR? ? OR DETECT? ? OR DETECTION OR INTRUD? OR INTRUSION OR RESPONSE OR ALERT? OR INCIDENT? ? OR INCIDENCE OR ATTACK? OR ANALY?S OR ANALYZE OR SENSORY(W) TECHNOLOGY OR FILTER

S3 10688 SURVEILLANCE OR CRYPTOGRAPH? OR TROJAN() HORSE OR FOOTPRINT? OR VULNERABIL?

S4 29478 (NETWORK OR NT) (1ON) SECURITY OR INTELLIGEN?() DATABASE? ? OR MANAGED() SECURITY() MONITORING OR SECURE(W) OPERATION? OR SECURITY(W) ANALYST OR SECURITY(W) ENGINEER OR NETWORK() ADMINISTRATOR OR DATABASE? ?

S5 764 S1 AND (S2 OR S3) AND S4

S6 5 S1 AND S2 AND S3 AND S4

?

00655199

INFRARED INTRUSION SENSOR

INFRAROTEINDRINGSSENSOR

CAPTEUR INFRAROUGE ANTI-INTRUSION

PATENT ASSIGNEE:

THE COMMONWEALTH OF AUSTRALIA, (512720), c/o the Secretary Department of Defence Support, Anzac Park West Building, Constitution Avenue, Canberra, Australian Capital Territory 2600, (AU), (Proprietor designated states: all)

INVENTOR:

LIDDIARD, Kevin, Charles, 18 Ferrier Avenue, Fairview Park, S.A 5126, (AU)

RICE, Brian, William, 14 Leabrook Street, Restrevor, S.A. 5073, (AU)

WATSON, Rodney, James, 30 Frances Avenue, Para Hills, S.A. 5096, (AU)

LEGAL REPRESENTATIVE:

de Bruijn, Leendert C. et al (19641), Nederlandsch Octrooibureau P.O. Box 29720, 2502 LS Den Haag, (NL)

PATENT (CC, No, Kind, Date): EP 630510 A1 941228 (Basic)

EP 630510 A1 960410

EP 630510 B1 991208

WO 9318492 930916

APPLICATION (CC, No, Date): EP 9305108 930308; WO 93AU93 930308

PRIORITY (CC, No, Date): AU 921228 920309

DESIGNATED STATES: BE; CH; DE; FR; GB; IT; LI; NL; SE

INTERNATIONAL PATENT CLASS: G08B-013/193; G08B-013/19; G08B-013/189;

G08B-013/183; G08B-013/181; G08B-013/18

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

| Available Text | Language | Update | Word Count |
|----------------|-----------|--------|------------|
| CLAIMS B | (English) | 9949 | 1188 |
| CLAIMS B | (German) | 9949 | 993 |
| CLAIMS B | (French) | 9949 | 1328 |
| SPEC B | (English) | 9949 | 3470 |

Total word count - document A 0

Total word count - document B 6979

Total word count - documents A + B 6979

...SPECIFICATION means adapted to display the output alarm signals.

In this arrangement a number of infrared **intrusion sensors** are preferably controlled from a central location by the network control means. Control may be...

...a commercially available personal computer. Alternatively, the sensors may be integrated with an existing remote **surveillance or security sensor** system.

In preference the **network** control means comprises a computer and network controller. The network controller interfaces between the plurality of infrared **intrusion sensors** and a serial port of the computer. In this arrangement the computer may also comprise...

5/3, K/4 (Item 1 from file: 349).

DIALOG(R) File 349:PCT Fulltext

(c) 2001 WIPO/MicroPat. All rts. reserv.

00800753

TESTING OF ACCESS SECURITY OF COMPUTERS ON A DATA COMMUNICATION NETWORK
TEST DE SECURITE D'ACCES D'ORDINATEURS SUR UN RESEAU DE COMMUNICATION DE
DONNEES

Search report

Patent Applicant/Assignee:

VIGILANTE A S, Vermundsgade 38, DK-2100 Copenhagen O, DK, DK (Residence),
DK (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

MUNKEDAL Ulf, Ryparken 39 St., DK-2100 Copenhagen O, DK, DK (Residence),
DK (Nationality), (Designated only for: US)

HEJGAARD VESTERGAARD Aage, Godsparken 164, DK-2670 Greve, DK, DK
(Residence), DK (Nationality), (Designated only for: US)

NORGAARD Bo, Sophienborgvaenget 9, DK-3400 Hillerod, DK, DK (Residence),
DK (Nationality), (Designated only for: US)

VARSTED Steen, Elmevang 28, DK-2830 Virum, DK, DK (Residence), DK
(Nationality), (Designated only for: US)

NEUPART Lars, Sveasvej 10, 3., 2, DK-1917 Frederiksberg C, DK, DK
(Residence), DK (Nationality), (Designated only for: US)

GRUNDL Peter, Edward Griegs Gade 17, 3. th., DK-2100 Copenhagen O, DK, DK
(Residence), DK (Nationality), (Designated only for: US)

WILLEN Ken, Geelsdalen 14, DK-2830 Virum, DK, DK (Residence), DK
(Nationality), (Designated only for: US)

Legal Representative:

PLOUGMANN VINGTOFT & PARTNERS A S (agent), Sankt Annae Plads 11, DK-1250
Kobenhavn K, DK,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200133353 A2 20010510 (WO 0133353)

Application: WO 2000DK616 20001103 (PCT/WO DK0000616)

Priority Application: DK 991584 19991103; US 99164332 19991109; DK
20001073 20000707

Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY
BZ CA CH CN CR CU CZ CZ (utility model) DE DE (utility model) DK DK
(utility model) DM DZ EE EE (utility model) ES FI FI (utility model) GB
GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KR (utility model) KZ LC LK
LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK
SK (utility model) SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 18162

Fulltext Availability:

Detailed Description

Detailed Description

... to determine the protocol for each of the open ports found by nmscan.

Internet Scanner NT : A commercial **security** scanner from ISS
(<http://www.iss.net>). It is used to scan for a lot of known
vulnerabilities .

Internet Scanner Linux: A commercial **security** scanner from ISS
(<http://www.iss.net>). It is used to...

5/3,K/5 (Item 2 from file: 349)

DIALOG(R) File 349:PCT Fulltext

(c) 2001 WIPO/MicroPat. All rts. reserv.

00799787 **Image available**

ARCHITECTURES FOR NETCENTRIC COMPUTING SYSTEMS

ARCHITECTURES DESTINEES A DES SYSTEMES INFORMATIQUES S'ARTICULANT AUTOUR

~~SECRET~~
Securite informatique utilisant un virus sondeur**PATENT ASSIGNEE:**

LCENT TECHNOLOGIES INC., (2143720), 600 Mountain Avenue, Murray Hill,
New Jersey 07974-0636, (US), (Applicant designated States: all)

INVENTOR:

Grosse, Eric, 140 North Road, Berkeley Heights, New Jersey 07922, (US)

LEGAL REPRESENTATIVE:

Watts, Christopher Malcolm Kelway, Dr. et al (37392), Lucent Technologies
(UK) Ltd, 5 Mornington Road, Woodford Green Essex IG8 OTU, (GB)

PATENT (CC, No, Kind, Date): EP 936787 A2 990818 (Basic)

APPLICATION (CC, No, Date): EP 99300332 990119;

PRIORITY (CC, No, Date): US 15563 980129

**DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE**

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-029/06

ABSTRACT WORD COUNT: 133

NOTE:

Figure number on first page: 1

LANGUAGE (Publication, Procedural, Application): English; English; English

FULLTEXT AVAILABILITY:

| Available Text | Language | Update | Word Count |
|------------------------------------|-----------|--------|------------|
| CLAIMS A | (English) | 9933 | 899 |
| SPEC A | (English) | 9933 | 4511 |
| Total word count - document A | | | 5410 |
| Total word count - document B | | | 0 |
| Total word count - documents A + B | | | 5410 |

...SPECIFICATION whether particular clients with a computer network are universally configured in accordance with the desired **network security** features of the computer **network**. More particularly, firewall 180 is configured, ...and thereafter virus probes are inserted at random intervals. Illustratively, probe 315 is a virus **probe in trojan horse** form, as previously discussed, wherein the insertion of probe 315 into file 305 results in...

...browser. Further, illustratively, "image1" is a unique string of characters for identifying probe 315. Basically, **probe** 315 is a **trojan horse** which directs the web browser to allocate an off-screen bitmap space, i.e., "new..."

...In accordance with the invention, if web browser 166 is in compliance with the illustrative **network security** feature which requires that all web browsers have their Javascript interpreter disabled, probe 315 will...

...a network resource, i.e., image1, unless it is improperly configured and outside of established **network security** measures. That is, execution of probe 315 means that web browser 166 is Javascript enabled which is not in compliance with the desired **security** measure of the private **network** 130 and therefore poses a **security** risk to the **network**.

As described previously, a further embodiment of the invention employs a UDP packet as the...

5/3,K/3 (Item 3 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2001 European Patent Office. All rts. reserv.

Search report

correlation, handle routine events and alert administrators to events needing immediate attention.

Frameworks Evolution Mimics Network Management's Path

Currently, early...sources. Reporting, historical analysis and automated response all benefit from event correlation. Event correlation for network security is no different--rules need to be developed to identify security events correctly while ignoring innocuous events.

The mainstay of any security system is its reporting and...whole. For example, Enterprise Security Manager, NetRecon, NetProwler and Intruder Alert will share the same vulnerability signature database , also slated for the second quarter. Check Point is building on OPSEC, integrating more partners...

10/3, K/10 (Item 4 from file: 13)
DIALOG(R) File 13:BAMP
(c) 2001 Resp. DB Svcs. All rts. reserv.

01111117 01834131 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Mapping a Network Security Strategy

(Developing principles and knowing the layout are the first 2 steps in ensuring that proper computer security policies are put in place and followed)

Article Author(s): Middleton, Bruce, BSEET

Security Management, v 43, n 2, p 79-85

February 1999

DOCUMENT TYPE: Journal ISSN: 0145-9406 (United States)

LANGUAGE: English RECORD TYPE: Fulltext, Abstract

WORD COUNT: 3565

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:

...with input from information systems personnel or other personnel responsible for any portion of the information stored on the network. They must also receive the full support of senior management. In addition

...

...disks between home and work. In companies where there is a great deal of proprietary information being stored on the network, some policies bar employees from bringing any diskettes from the outside. Others...for the company.

Network intrusion. Among the most common defensive tools being implemented on computer networks today are intrusion detection systems (IDS). Generally, when evaluating these systems, the security manager should be looking for those that automatically alert IS personnel via pager, e-mail, telephone, or console to potential intruders into the network domain. The intrusion detection system should provide "exception" reports when something out of the ordinary occurs. The security manager... as some Web sites that provide helpful information on threats and technologies.

Auditing Systems

* Kane Security Analyst ; Kane Security Monitor Security Dynamics Technologies, Inc. 800/SECURID www.securitydynamics.com

Search report

* ISS SafeSuite Internet Security Systems 678/443...

...sun.com/pubcgi/pubpatches.html

* Internet Security Systems Vulnerability Alert http://www.iss.net/xforce/alerts/advise8.html

Incident Response

* COAST (Purdue University) http://www.cs.purdue.edu/coast/ coast.html

* CERT Summary http://www...

10/3, K/11 (Item 5 from file: 13)

DIALOG(R) File 13:BAMP

(c) 2001 Resp. DB Svcs. All rts. reserv.

01077561 01414864 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Protecting against attacks on open systems

(Attacks on open control systems can come from viruses, network stack attacks, Trojan horses and many other sources)

Article Author(s): Dalrymple, Philip W, III

Instrumentation & Control Systems, v 71, n 2, p 51-55

February 1998

DOCUMENT TYPE: Journal ISSN: 1074-2328 (United States)

LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 3305

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:

...sending packets that are not in compliance with Internet standards will not cause any problems.

* Network security monitors --A network security monitor is a protocol analyzer with software that looks for problems--not with the communication protocol, but with the security on the systems. These are very useful tools for the early detection of security problems. However, they do have one drawback: a network security monitor needs to see each of the packets that goes across your network. With old-style...

...all of the information that it needs to do its job.

In any case, a network security monitor should be available and it should be used regularly.

Anti-virus software

Anti-virus software...software is wrong about which virus it has found, the disinfecting process can damage the information stored on a system. Then, too, the virus itself may have a bug in it. If...

...other Acme locations were avoided by disconnecting the corporate network connection until the problem was resolved.

FBN had intentionally sent a broadcast ping of death and a number of ICMP redirect packets into the plant...have an operating system that is a popular target for where virus-based attacks.

...track trends and generate reports. ISS's ePatrol Managed Intrusion Detection service, for instance, can **store information** on events in a Microsoft Access and SQL relational **database**. A tool or service can also be customized to automatically shut down a particularly sensitive port if...

...service attacks on Amazon.com, CNN and Yahoo in February boosted awareness--and business--for **intrusion detection** technology, which basically acts as a burglar alarm on the **network**.

Security experts say the next round of hacker attacks will be more deadly, potentially taking...

...and the internal corporate security threats are covered by the **intrusion tools**.

"A combination of **network** and host-based-**intrusion detection** is critical. If you just do one or the other, you are missing half of..."

...own intrusion detection and hiring an **outsourcer** is manpower and expertise. When intrusion detection is **handled** in-house, the **alarms** can be overwhelming.

"When an alarm sounds, no one knows what to do with it...The Depository Trust Co. in New York, which uses IBM Global Services to handle the **intrusion detection** at the entry points of its **network**, and its own Axent NetProwler detection tools for watching the inside of the network.

"The..."

...of-service attack, but they can at least give a heads-up if one is **infiltrating** a **network**.

"**Intrusion detection** shouldn't provide a false sense of security," says Found-stone's Kurtz. "There are..."

...operations for Pilot.

Even with an intrusion detection service, there's always the risk of **hackers** shutting down the **sensors** so they can sneak into the **network**, says Depository Trust's Jarocki. That's why risk management and regular audits by white now, here are some of the intrusion detection services available today:

* Pilot Network Services offers an overall secure IP **network** service with **intrusion detection** built in. Pilot's proprietary Heuristic Defense Infrastructure technology "learns" from past network events and...

...Pilot's own security technicians, who analyze network traffic. All three of Pilot's main **network** services--secure Internet, secure hosting and VPN--come with **intrusion detection**. As with any secure IP **network** service, the catch is that you have to be a Pilot subscriber. Pilot's secure...

...fee for 400 users, plus \$1,000 per month.

* IBM Global Services has been offering **network intrusion detection** services for three years as part of its consulting, vulnerability and virus services. Michael Puldy...

...month, DefendNet will put a firewall on a company's site and handle all

Search report

Fogarty, Kevin
Network World v11n20 PP: 38 May 16, 1994
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 385

...TEXT: databases support only one compiler, according to Banks. By supporting more than one, Versant's **database** can **handle** objects created in different formats that would otherwise be incompatible, he said.

MANAGING INFORMATION

Using...

...Rymer, analyst with the Boston-based Patricia Seybold Group, Inc.

That is because an object **database** can **handle** complex data structures, including compound documents, financial or performance models, and other data types that...

... help it manage its international network. The telephone giant will use Versant to store and **filter** **network** **alarms**, **handle** **event** reporting and **track** performance management, according to Andrew Jacobs, chief of **network** management for MCI in Colorado Springs.

Versant pricing ranges from \$5,000 to \$10,000...

10/3,K/5 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2001 Bell & Howell. All rts. reserv.

00746222 93-95443

Taking control

Carleton, Mary; Capen, Tracey
InfoWorld v15n28 PP: 58-69 Jul 12, 1993
ISSN: 0199-6649 JRNL CODE: IFW
WORD COUNT: 11172

...TEXT: and network printers, a DOS File Manager, an administrator's to-do list, and a **virus** **checker**. **LAN** Workstation is **network** independent. It runs on all popular PC-based LANs.

XTree Tools for Networks: XTree Tools...can display as many customizable real-time graphs as your PC's screen, CPU, and **memory** can **handle**. Each graph displays up to 50 minutes of continuous activity. Most NetWare statistics can be...

...off. If you click on an alarm icon, it gives you a description of the **alarm** and suggested **responses**. **Alarms** can simply be logged, they can beep until acknowledged, they can display as a tickertape...

... WORKSTATION: Saber's network monitoring is thin. It gives you a utility to run scheduled **network** jobs, such as **virus** **checking** or scheduled backups. Using custom scripts, **LAN** Workstation's Event Logger can log nearly any event on the network. There is also...the standard system configuration files. Packages that automatically logged detectable hardware changes and kept a **database** with detailed **information** about each workstation earned a good score. Better packages provided filters for viewing the database...

...it and sends a network system message to the administrator.

With the introduction...7848.

CIRCLE 613 ON READER CARD

RELATED ARTICLE: UNATTENDED BACKUP, NEAR-LINE ARCHIVE AND DATA

STORAGE

Management **solutions** for UNIX Platforms, Client/Servers and Networks of Heterogeneous Systems

Herstal has been a leading supplier of hardware/software **solutions** for Hierarchical **Storage** Management (HSM) for 15 years. Herstal began as a manufacturer of third party memory for...

...line and optical disk robotic autochangers by developing operational software solutions.

Today, Herstal offers data **storage** manmanagement software **solutions** which range from device drivers and operator automation programs to UNIX enterprise system management. Herstal's data **storage** management software **solutions** are complemented by a full line of data storage hard-products -- from memory upgrades to...

10/3,K/7 (Item 1 from file: 13)

DIALOG(R)File 13:BAMP

(c) 2001 Resp. DB Svcs. All rts. reserv.

01169081 02484536 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Human Element Is Key To Stopping Hackers

(Internet security is key for today's business world, but the human element is just as important; article explains how only a person can detect the difference between a security breach and an innocent mistake)

Article Author(s): Higgins, Kelly Jackson

Information Week, p 164, 166+

May 29, 2000

DOCUMENT TYPE: Journal ISSN: 8750-6874 (United States)

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 2504

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:

...ATTACKS BECOME MORE FREQUENT AND DAMAGING

It was 2 a.m. when the intrusion-detection **alarm** sounded at DefendNet **Solutions** Inc. Security technicians at the managed-security services firm scrambled to find the source of...

...outside experts who collate and sift through all the information, superfluous or not, generated by **intrusion -detection sensors** sitting on a **network**. These services manage all the hardware and software tools, too. Companies typically pay a monthly...

...private networks (VPN). Companies such as DefendNet, IBM Global Services, Internet Security Systems (ISS), Pilot **Network** Services, and RIPTech already offer **intrusion -detection** services. Other **security** companies, including Axent Technologies Inc., plan to roll them out soon. The market for managed...

...are under pressure to place full-time monitoring tools at the hot spots in their **networks** to continuously sniff out and deter intruders.

An **intrusion -detection** tool works much like an antivirus package. Sensors look for known "signatures," or potential hacker...

...to track trends and generate reports. ISS's ePatrol Managed Intrusion Detection service, for instance, **stores information** on events in a Microsoft Access and SQL relational **database**. A **tool** or service can also be customized to automatically shut down a particularly sensitive port if...

...sites such as Amazon.com, CNN, and Yahoo in February boosted awareness--and business--for **intrusion -detection** technology, which basically acts as a burglar alarm on the **network**.

photo omitted

Security experts predict that the next round of hacker attacks will be more ...

...as the internal corporate security threats are covered by the **intrusion tools**. "A combination of **network** - and host-based **intrusion detection** is critical," says George Kurtz, CEO of Foundstone Inc., a security consulting firm. "If you..."

...intrusion detection and hiring an **outsourcing** company are manpower and expertise. When intrusion detection is **handled** in-house, the **alarms** can be overwhelming. "When an alarm sounds, no one knows what to do with it..."

...is outsourcing everything, including the network, Web servers, and security technology. The ASP uses Pilot **Network Services**' VPN service, which comes with **intrusion detection** built in. "We don't have an infrastructure--Pilot hosts it," says Arun Shrestha, CEO...Take the Depository Trust Co. in New York, which uses IBM Global Services to handle **intrusion detection** at the entry points of its **network**, and Axent's NetProwler detection tools for watching the inside of the network.

photo omitted...

...of-service attack, but they can at least give a heads up if one is **infiltrating** a **network**.

"**Intrusion detection** shouldn't provide a false sense of security," Foundstone's Kurtz says. "There are still..."

...you're going to get infected," says Frank Swift, manager of security operations at Pilot **Network Services**.

Even with an **intrusion -detection** service, there's the risk of **hackers** shutting down the **sensors** so they can sneak into a **network**, says Depository Trust's Jarocki. That's why risk management and regular audits by white...Kovar, a program manager at consulting firm the Yankee Group.

Here are some of the **intrusion -detection** services available today:

* Pilot **Network Services** Inc. offers an overall secure IP **network** service with built-in **intrusion detection**. Pilot's proprietary Heuristic Defense Infrastructure technology "learns" from past **network** events and applies that knowledge when it takes action or does other tracking. HDI runs...

...All three of Pilot's main network services--secure Internet, secure hosting, and virtual private **networks**--come with **intrusion detection**. As with any secure IP **network** service, the catch is that you have to be a Pilot subscriber. Pilot's secure...

...month, DefendNet will put a firewall on a company's site and handle all

Search report

File 15:ABI/Inform(R) 1971-2001/May 29
(c) 2001 Bell & Howell
File 88:Gale Group Business A.R.T.S. 1976-2001/May 30
(c) 2001 The Gale Group
File 635:Business Dateline(R) 1985-2001/May 26
(c) 2001 Bell & Howell
File 9:Business & Industry(R) Jul/1994-2001/May 25
(c) 2001 Resp. DB Svcs.
File 13:BAMP 2001/May W3
(c) 2001 Resp. DB Svcs.
File 624:McGraw-Hill Publications 1985-2001/May 30
(c) 2001 McGraw-Hill Co. Inc
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 610:Business Wire 1999-2001/May 30
(c) 2001 Business Wire.
File 647:CMP Computer Fulltext 1988-2001/May W4
(c) 2001 CMP
File 275:Gale Group Computer DB(TM) 1983-2001/May 29
(c) 2001 The Gale Group
File 674:Computer News Fulltext 1989-2001/May W3
(c) 2001 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2001/May 29
(c) 2001 The Dialog Corp.
File 98:General Sci Abs/Full-Text 1984-2001/Apr
(c) 2001 The HW Wilson Co.
File 47:Gale Group Magazine DB(TM) 1959-2001/May 29
(c) 2001 The Gale group
File 75:TGG Management Contents(R) 86-2001/May W3
(c) 2001 The Gale Group
File 570:Gale Group MARS(R) 1984-2001/May 29
(c) 2001 The Gale Group
File 239:Mathsci 1940-2001/Jul
(c) 2001 American Mathematical Society
File 621:Gale Group New Prod.Annou.(R) 1985-2001/May 29
(c) 2001 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2001/May 29
(c) 2001 The Gale Group
File 369:New Scientist 1994-2001/May W2
(c) 2001 Reed Business Information Ltd.
File 484:Periodical Abstracts Plustext 1986-2001/May W3
(c) 2001 Bell & Howell
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 16:Gale Group PROMT(R) 1990-2001/May 29
(c) 2001 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 141:Readers Guide 1983-2001/Apr
(c) 2001 The HW Wilson Co
File 634:San Jose Mercury Jun 1985-2001/May 27
(c) 2001 San Jose Mercury News
File 148:Gale Group Trade & Industry DB 1976-2001/May 29
(c) 2001 The Gale Group
File 553:Wilson Bus. Abs. FullText 1982-2001/Apr
(c) 2001 The HW Wilson Co
File 20:World Reporter 1997-2001/May 30
(c) 2001 The Dialog Corporation

Set Items Description

Sep 15, 1996

DOCUMENT TYPE: Buyers Guide

ISSN: 1069-5621

LANGUAGE: English

RECORD TYPE: Fulltext; Abstract

WORD COUNT: 27890 LINE COUNT: 02386

...ABSTRACT: is presented. Categories include Cable Testing Equipment; Help Desk; Inventory, Software Metering and Asset Management; **Network Management Applications**; Network Management Platforms; Probes and **Monitors**; Protocol **Analyzers**; **Security**; Server Management; Server Room/Wiring Closet Accessories; Storage Management Software; Tape-Backup Hardware; Training; and...

... LAN Server, VINES, and Windows NT networks. It supports call tracking, trouble ticketing, problem routing, **knowledge base**, and reporting features. The price starts at \$1,595 for 2 users.

MCAFEE VYCOR ENTERPRISE...when the application becomes available. It costs \$50 per node in quantity.

INTERPOSE CLIENT/SERVER SOLUTION ADVISER

Client/Server Solution Adviser, designed for NetWare 3.x, NetWare 4.x, LAN Manager, and Windows NT networks, automatically...functions and supports SNMP. Data is stored in an Ingres database. The product provides **on-screen** and e-mail **event** notification. The price is \$4,995.

ASCOM TIMEPLEX SYNCHRONY NETWORK MANAGEMENT SYSTEM

Synchrony Network Management System manages WAN switches and Synchrony ST-1000 on HP...sign-on functions. Data is stored in a proprietary database, and the product provides **on-screen event** notification.

CLEAR COMMUNICATIONS CLEARVIEW

Clearview manages DSUs and **WAN** switches on HP OpenView, HP/UX, Solaris, and SunOS management platforms. It provides fault management and performance management functions. Data is stored in a Sybase database. The product provides **on-screen** and pager **event** notification. Prices vary depending upon configuration.

COMMUNICATION DEVICES NETWORK WINDOWS

Network Windows manages dial-up modems on DOS/Windows management platforms using a Windows interface. It...

...and supports SNMP Data is stored in a management platform database. The product provides **on-screen event** notification. The price is \$395.

DATUM TYMSERVE 2000 NETWORK TIME SERVER

Tymserve 2000 Network Time Server manages NTP using an SNMP interface. It provides...and supports SNMP; Data is stored in a management platform database. The product provides **on-screen event** notification and costs \$5,000.

GENERAL SIGNAL NETWORKS DELIVER IT Deliver It! provides electronic software distribution and asset management functions. It runs on...Data is stored in a management platform database or proprietary database. The product provides **on-screen event** notification. Prices start at \$495.

NEON SOFTWARE LAN SURVEYOR

LAN Surveyor works with AppleShare and manages routers and end-nodes using a MacOS interface. It...and supports SNMP. Data is stored in management platform database, and the product provides **on-screen event** notification and costs \$600.

RAD NETWORK DEVICES MULTIVU/OV/6000

MultiVu/OV/6000 works with Unix and manages bridges/switches and... ...and supports SNMP. Data is stored in a management platform database. The product provides **on-screen event** notification and costs \$3,995.

RAD NETWORK DEVICES MULTIVU/WIN

MultiVu/Win works with NetWare 3.x and NetWare 4.x and...

...SNMP and SNMP-2. Data is stored in a proprietary database. The products

Search report

outers, switches, workstations, firewalls, Web servers, and other network devices. The product features extensive graphs...

...com

ODS Networks
Computer Misuse Detection System 4.0
www.ods.com
Security Dynamics
Kane **Security Analyst**, Kane **Security Monitor**
www.securitydynamics.com
Tripwire Security Systems
Tripwire for Unix, Windows NT
www.tripwiresecurity.com

10/3,K/22 (Item 5 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

02195139 SUPPLIER NUMBER: 20888299 (USE FORMAT 7 OR 9 FOR FULL TEXT)

CyberCop Scans And Protects The Perimeter. (Network Associates Inc's CyberCop Scanner 2.4) (Software Review) (Evaluation)

Phillips, Ken

PC Week, v15, n27, p93(1)

July 6, 1998

DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 1979 LINE COUNT: 00164

... addition, CyberCop Scanner can perform password cracking and "brute force" password guessing, denial-of-service **attacks**, packet **filter** integrity **checks**, and even help advanced users construct custom-designed test packets.

Exposed vulnerabilities

The 2.4...

...real-time intruder detection and network abuse (content monitoring), are not within its purview.

However, Network Associates does offer a separate product for **intrusion detection**, called CyberCop Network (see PC Week Labs' review, April 20, Page 89), plus CyberCop Server for securing Web...

...level detail about which applications or commands to run to fix the problem.

Computer Emergency Response Team **advisory** and Microsoft **Knowledge Base** references were also few, so administrators are likely to feel largely on their own after...in the CyberCop Scanner.

PC Week Labs Executive Summary: CyberCop Scanner 2.4

Enterprise administrators looking to increase **network security** should consider CyberCop Scanner, a flexible, feature-rich product for auditing vulnerability to external threats...

10/3,K/23 (Item 6 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2001 The Gale Group. All rts. reserv.

01989476 SUPPLIER NUMBER: 18684483 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Network management. (1996 Buyers Guide) (Buyers Guide)
LAN Magazine, v11, n10, p201(52)

Search report

attacks in progress. Also, because network-based products actually look at packet headers...no universal method currently exists for IDS products to communicate with each other and with **network** -management systems. The IETF recently formed the **Intrusion Detection** Exchange Format Working Group, which works on defining data formats and exchange protocols for sharing...

...just about every enterprise has at least one firewall to protect various segments of the **network**. But these same companies may be low on the **intrusion -detection** education curve. However, this hasn't stopped the market from taking off.

The Hurwitz Group...

...software from the original manufacturer.

BEING A GOOD HOST

One vendor in the host-based **intrusion -detection** space is ODS Networks (Richardson, TX), which in March 1999 began shipping version 4.0 of its Computer Misuse...

...night login attempts and an increase in file browsing on a server.

Another host-based **intrusion -detection** system is **Network** Associates' CyberCop Server, which runs on Windows NT 4.0 as well as Sun Microsystems attacks while they are in progress.

WHO'S WATCHING THE **NETWORK** ?

Host-based **intrusion -detection** systems are crucial for detecting sometimes subtle changes within servers that could signal intruders within

...

...horses, changes to Unix kernels, Satan, buffer overflows, system configuration changes, and Ping flooding.

Another **network** -based **intrusion -detection** product is Cisco's NetRanger, a product that came from the company's acquisition of...

...exactly where the attack is taking place and how serious it is. The product's **database of information** contains countermeasures and other facts about attacks.

When Memco Software acquired AbirNet last year, it...

...manages enterprise security from a single location. It rolls policy management, vulnerability assessment (much like **network** scanners), and host-based **intrusion detection** into one. Entrax supports Solaris and Windows NT and includes 41 Unix assessments and 27...

...and hoping for the best, you can add ever-vigilant eyes and ears to your **network security** with **intrusion detection**.

Anita Karve

a, associate editor, can be reached at akarve@mfi.com.

An excellent place...Scanner is one of the more popular tools on the market. The product conducts automatic **network scans** and **looks** for **security** holes using a database of known attacks. It can evaluate weaknesses of an entire enterprise...

...Dynamics' (Bedford, MA) Kane Security Analyst, which the company obtained through its 1998 acquisition of **Intrusion Detection**. This product **checks** Windows NT and Novell NetWare **networks** for unused user accounts and IDs, password compliance with the security policy, the installation of...

...to what.

Cisco Systems' acquisition of Wheel Group yielded a scanner product called NetSonar, which **looks** for **security** problems by **analyzing**

industry's "preferred solution for network vulnerability analysis and decision support".

M2 Presswire, pNA

April 18, 2000

Language: English Record Type: Fulltext

Document Type: Magazine/Journal; Trade

Word Count: 725

...succession; SC praises ISS's pioneering scanner technology as the industry's "preferred solution for network vulnerability analysis and decision support".

... automatically tests networks from a security perspective using the industry's most comprehensive database of **detection** methods. Internet Scanner scans **network** devices to **detect vulnerabilities**, prioritises **security** risks and generates a wide range of reports ranging from executive-level analysis to detailed...

16/3,K/22 (Item 2 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

(c) 2001 The Gale Group. All rts. reserv.

03909909 Supplier Number: 50111864 (USE FORMAT 7 FOR FULLTEXT)

ISS: ISS's Internet Scanner awarded " Network Security Product of the Year" at UK networking event

M2 Presswire, pN/A

June 29, 1998

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 689

(USE FORMAT 7 FOR FULLTEXT)

ISS: ISS's Internet Scanner awarded " Network Security Product of the Year" at UK networking event

TEXT:

...voted the "Best Security Management Product" by readers of Secure Computing magazine in April, Internet **Scanner**, the market-leading **network vulnerability detection** software from Internet **Security** Systems, has won yet another major accolade. Internet **Scanner**, the industry's first security scanning product, was honoured by a panel of networking experts...

16/3,K/23 (Item 3 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

(c) 2001 The Gale Group. All rts. reserv.

03828168 Supplier Number: 48313090 (USE FORMAT 7 FOR FULLTEXT)

INTERNET SECURITY SYSTEMS: ISS takes the pain out of finding and fixing network security problems

M2 Presswire, pN/A

Feb 24, 1998

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 860

INTERNET SECURITY SYSTEMS: ISS takes the pain out of finding and fixing network security problems

... utilises a powerful, industry-unique security engine containing a comprehensive and dynamic database of **attacker** methods and **security**

Search report

Scanner 5.6 network security software) (Brief Article) (Product Announcement)

ENT, 4, 3, 26(1)

Feb 3, 1999

DOCUMENT TYPE: Brief Article Product Announcement

ISSN: 1085-2395

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 143 LINE COUNT: 00017

ISS Adds SmartScan to Internet Scanner. (Internet Security Systems' Internet Scanner 5.6 network security software) (Brief Article) (Product Announcement)

TEXT:

Internet Security Systems Inc. (ISS) released the network security vulnerability detection software Internet Scanner 5.6. The new version has SmartScan technology and 85 new detection methods for identifying...

16/3,K/14 (Item 4 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2001 The Gale Group. All rts. reserv.

02250609 SUPPLIER NUMBER: 53363073 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Network Associates Announces New, Faster Firewall 12/06/98.

Newsbytes, NA

Dec 7, 1998

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 241 LINE COUNT: 00025

Network Associates Announces New, Faster Firewall 12/06/98.

... adaptive proxy technology also enables more flexible integration between individual security products such as security vulnerability scanners, virus security scanners and intrusion protection sensors

Network Associates' initial benchmark tests showed a tenfold or greater performance improvement with zero security compromise...

16/3,K/15 (Item 5 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2001 The Gale Group. All rts. reserv.

02201484 SUPPLIER NUMBER: 20941474 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Security Specialist puts scanner on Web on Web. (Internet Security Systems' Internet Scanner 5.2 network vulnerability detection software) (Product Announcement)

Computer Weekly, p40(1)

July 9, 1998

DOCUMENT TYPE: Product Announcement

ISSN: 0010-4787

LANGUAGE:

English RECORD TYPE: Fulltext

WORD COUNT: 48 LINE COUNT: 00007

Security Specialist puts scanner on Web on Web. (Internet Security Systems' Internet Scanner 5.2 network vulnerability detection software) (Product Announcement)

16/3,K/16 (Item 6 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

ability to tailor their output.

Internet Scanner continues its position as the most comprehensive network security vulnerability detection solution with the integration of many new, significant Windows NT and UNIX vulnerability checks, including...

16/3,K/6 (Item 5 from file: 810)

DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0734051 BW1079

ISS: ISS' SAFEsuite Network Security Assessment and Monitoring Tools Now Available On Unisys SEWP II Contract

August 12, 1997

Byline: Business Editors/Computer Writers

ISS' SAFEsuite Network Security Assessment and Monitoring Tools Now Available On Unisys SEWP II Contract

...security holes, and monitors network traffic around-the-clock in real-time, looking for network attack patterns and stopping network break ins Scanner (TM) - the leading network security assessment tool for detecting and analyzing network security vulnerabilities ; System Security Scanner (TM) - a security assessment tool for identifying security weaknesses in host systems; and RealSecure(TM...)

16/3,K/7 (Item 6 from file: 810)

DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0719464 BW0093

INTERNET SECURITY SYS: Internet Security Systems ships new version of leading network security assessment tool

July 01, 1997

Byline: Business Editors/Computer Writers

Internet Security Systems ships new version of leading network security assessment tool

...issues across an entire network of Unix, Windows NT and Windows 95 machines. The tool probes a network and automatically detects potentially harmful security vulnerabilities using the industry's most comprehensive penetration tests.

In addition to checking for the IIS...

...number of network security vulnerabilities and threats.

The Atlanta-based company's flagship product, Internet Scanner , is the leading commercial attack simulation and security auditing

Search report

tool used to eliminate **network security vulnerabilities** in corporations, financial institutions, and government agencies worldwide including 9 out of the top 10...

16/3,K/8 (Item 7 from file: 810)
DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0717732 BW1398

INTERNET SECURITY SYS: ISS helps universities face the challenges of network security

June 25, 1997

Byline: Business Editors/Computer Writers

ISS helps universities face the challenges of network security

...number of network security vulnerabilities and threats.

The Atlanta-based company's flagship product, **Internet Scanner**, is the leading commercial attack simulation and **security** auditing tool used to eliminate **network security vulnerabilities** in corporations, government agencies and financial institutions worldwide including 9 out of the top 10...

16/3,K/9 (Item 8 from file: 810)
DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0711428 BW0247

INTERNET SECURITY SYS: Internet Security Systems helps network professionals capitalize on growing information security market

June 09, 1997

Byline: Business Editors/Computer Writers

Internet Security Systems helps network professionals capitalize on growing information security market

...number of network security vulnerabilities and threats.

The Atlanta-based company's flagship product, **Internet Scanner**, is the leading commercial attack simulation and **security** auditing tool used to eliminate **network security vulnerabilities** in corporations, financial institutions and government agencies worldwide including nine out of the top 10...

16/3,K/10 (Item 1 from file: 647)
DIALOG(R) File 647:CMP Computer Fulltext
(c) 2001 CMP. All rts. reserv.

01192371 CMP ACCESSION NUMBER: IWK19990524S0052
CyberCop Patrols On Linux - Network Associates Scanner Detects

Conference Title: IMCS-7: 7th International Meeting on Chemical Sensors
Publication Year: 2000

15/6/11 (Item 3 from file: 8)
05012171

Title: Distributed events in active database systems: letting the genie out of the bottle
Publication Year: 1998

15/6/12 (Item 4 from file: 8)
05005594

Title: Turning the lights back on in the data centre
Conference Title: Proceedings of the 1997 23rd International Conference for the Resource Management & Performance Evaluation of Enterprise Computing Systems. Part 1 (of 2)
Publication Year: 1997

15/6/13 (Item 5 from file: 8)
04919316

Title: Intelligent database for engineering applications
Publication Year: 1998

15/6/14 (Item 6 from file: 8)
04575689

Title: Formal semantics for an active functional DBPL
Publication Year: 1996

15/6/15 (Item 7 from file: 8)
04477998

Title: MIB for video server system management
Conference Title: Proceedings of the 1996 2nd International Workshop on Community Networking
Publication Year: 1995

15/6/16 (Item 8 from file: 8)
03796638

Title: Real-time decision-support system for freeway management and control
Publication Year: 1994

15/6/17 (Item 9 from file: 8)
02258361

Title: FRESH: A NAVAL SCHEDULING SYSTEM.
Conference Title: Proceedings - The Third Conference on Artificial Intelligence Applications.
Publication Year: 1987

15/6/18 (Item 1 from file: 34)

09251930 Genuine Article#: 385AA Number of References: 38

Title: Brain responses to nouns, verbs and class-ambiguous words in context
(ABSTRACT AVAILABLE)

Publication date: 20001200

15/6/19 (Item 2 from file: 34)

05739904 Genuine Article#: WU487 Number of References: 39

Title: RBE: A rule-by-example active database system (ABSTRACT AVAILABLE)
Publication date: 19970400

15/6/20 (Item 1 from file: 35)
01706876 ORDER NO: AADMQ-37578

ACTIVECBR: INTEGRATING CASE-BASED REASONING AND ACTIVE DATABASES
Year: 1998

15/6/21 (Item 2 from file: 35)
01226068 ORDER NO: AAD92-19439

APPLICATION OF KNOWLEDGE-BASED EXPERT SYSTEMS TO INCIDENT MANAGEMENT ON
FREEWAYS
Year: 1992

15/6/22 (Item 1 from file: 144)
14769881 PASCAL No.: 00-0448981

Cycle mining in active database environments
Data mining and knowledge discovery : theory, tools, and technology II :
Orlando FL, 24-25 April 2000
2000

Copyright (c) 2000 INIST-CNRS. All rights reserved.

15/6/23 (Item 1 from file: 202)
00204832 9604832

ISA Document Number in Printed Publication: 9604478
Networked reproduction apparatus with security feature.
Document Type: Patent
Publication Year: 1996

15/6/24 (Item 1 from file: 233)
00552952 99SU11-005

What you need to know about NAS
19991101

15/6/25 (Item 2 from file: 233)
00546732 99IX09-001

Life after IDS -- You spent months evaluating, testing, purchasing and
deploying your intrusion detection system. Now the fun really begins
19990901

15/6/26 (Item 3 from file: 233)
00474981 97PK10-202
Intel revamps LDMS management suite
19971020

15/6/27 (Item 4 from file: 233)
00463407 97ID06-001
Avoiding computer viruses
19970601

15/6/28 (Item 5 from file: 233)
00373721 95IF01-005
Scanning for antivirus products -- Users have many choices and much
confusion
19950101

15/6/29 (Item 6 from file: 233)

Inside the Internet , June 1, 1997 , v4 n6 p1-3, 3 Page(s)
ISSN: 1075-7902

Explains what a **computer** virus is, how they spread, the various types, how to detect them, and how to avoid them. States that the first virus appeared in 1981, since which viruses have become more sophisticated and destructive. Defines a virus and explains that there are two basic methods for spreading viruses - travel with executable files and travel in the boot section of a floppy disk. Describes forms of viruses that make them hard to detect and macro viruses . Also discusses software that is available for detecting viruses , including virus shields, file integrity checkers , and anti-virus scanners . Says that signs of a virus include missing data files ; corrupted information ; system crashes; and computer slowdowns, which may also signify a software bug. Offers tips for avoiding viruses . Includes one screen display and two tables. (bjp)
?t15/7/28

15/7/28 (Item 5 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2001 Info. Today Inc. All rts. reserv.

00373721 95IF01-005

Scanning for antivirus products -- Users have many choices and much confusion

Ford, Richard
Info Security News , January 1, 1995 , v6 n1 p38-41, 4 Page(s)
ISSN: 1051-2500

Describes software solutions for detecting and removing computer viruses from information systems. Provides detailed descriptions and limitations of the following: scanners, NetWare Loadable Modules (NLM), integrity checkers , virus -behavior blockers, disk-validation products, and file immunization. Includes vendor contact information. Contains the sidebar ``The Virus from Hong Kong: A Case History'' (p39) by John Zimmerman narrating how the ``V-Sign'' computer virus infiltrated his company's management information system. Includes two drawings. (ACD)
?

Abstract: The author describes the basic elements and systematic process developed at Duke Power Company for determining recurring events and recurring problems. The first basic element used to support this process is the problem investigation report (PIR) program. The PIR program serves as the mechanism by which US Nuclear Regulatory Commission (NRC) reportable and nonreportable events and problems are identified, investigated, and resolved. The second basic element used to support this process is the in-house operating experience (OE) computerized data base. This data base contains information specific to each event and designed to facilitate data manipulation and sorting. Finally, the recurring event/problem guideline has been developed to systematically lead the user through the process using the PIR and OE programs. He very briefly describes the PIR data-handling process and summarizes the major changes to the process over the past 3 yr. Particular focus is on the recurring event/problem determination process. (0 Refs)

Subfile: A

15/7/4 (Item 4 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2001 Institution of Electrical Engineers. All rts. reserv.

03287069 INSPEC Abstract Number: C89005422

Title: Office automation security: closing the doors to your computer system

Author(s): Clyde, R.A.

Author Affiliation: Clyde Digital Syst., Orem, UT, USA

Conference Title: Proceedings of the Digital Equipment Users Society USA Fall 1987 p.209-13

Editor(s): Snyder, J.M.

Publisher: Digital Equipment Comput. Users Soc, Marlboro, MA, USA

Publication Date: 1987 Country of Publication: USA 346 pp.

Conference Date: 7-11 Dec. 1987 Conference Location: Anaheim, CA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Since today's organizations store information assets on computer systems, it is essential that an organization safeguard its computer systems. Eighty-seven percent of security problems comes from current or former employees, while only 13% comes from outsiders. This implies that an effective security system must solve the problem for insiders as well as outsiders. There are numerous common oversights that leave open doors to a computer system. The ways to correct these oversights include having sufficient physical and media security, properly managing passwords, controlling unattended logged-in terminals, using sufficient access controls, immediately applying software updates defending against Trojan horse attacks, and continually monitoring the system for security problems. (13 Refs)

Subfile: C

15/7/5 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2001 Institution of Electrical Engineers. All rts. reserv.

03142936 INSPEC Abstract Number: C88034873

Title: Worms in the field (CACL)

Author(s): Abbott, D.

Author Affiliation: Comput. & Aerosp. Components Ltd., Chessington, UK

Journal: Electronic Library vol.5, no.6 p.332-5

Publication Date: Dec. 1987 Country of Publication: UK

CODEN: ELLIDZ ISSN: 0264-0473

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Computer and Aerospace Components Ltd (CACL) markets the Intelligent Archive family of products based around a Worm optical disc drive, comprising (besides the Worm) an image scanner, text retrieval,

OCR and image-handling software. From its first sale to Channel 4 Television in June 1986, CACL has continued to implement its range of systems in a wide variety of blue-chip companies and government departments. CACL probably has more experience than anyone of Worm-based applications and presents its view of the marketplace and several client case studies. (0 Refs)

Subfile: C

15/7/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2001 Institution of Electrical Engineers. All rts. reserv.

00574061 INSPEC Abstract Number: C73023892
Title: Data migration and staging facility
Author(s): Brawn, B.; Hildebrand, D.B.
Journal: IBM Technical Disclosure Bulletin vol.16, no.1 p.205-8
Publication Date: June 1973 Country of Publication: USA
CODEN: IBMTAA ISSN: 0018-8689
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: A supervisorial controller is illustrated for automatic administration and control of a computer system's secondary storage resources, during the normal operation of the computer system. The Migration/Staging Monitor responds to events from many interfaces, to control the occurrence of general migration, immediate migration, and staging. (0 Refs)

Subfile: C

15/7/7 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS
Comp&distr 2000 NTIS, Intl Cpyrght All Right. All rts. reserv.

2140588 NTIS Accession Number: PB99-502072/XAB
Operational Information Systems Security (OISS), Volume 1 and 2 (on CD-ROM)
(Data file)
Defense Information Systems Agency, Falls Church, VA.
Corp. Source Codes: 111186000
Aug 1998 CD-ROM
Languages: English
Journal Announcement: GRAI9925
Requires Windows 95, 98, or NT, 16-bit sound card, 3 MB free space on hard drive. This is an interactive multimedia training CD-ROM. It was an EMMA Award nominee.

The datafile is on two CD-ROM discs. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703) 605-6000 (other countries); fax at (703) 605-6900; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: CD-ROM \$45.00

Country of Publication: United States

This interactive CD-ROM provides the user with an introduction to OISS, including its definition, evolution, and legal and regulatory issues associated with OISS. Topics covered include threats to Information Systems Security, examples of security violation, incident indicators and reporting procedures, Trusted Systems, and the certification and accreditation of systems. The roles and responsibilities of the ISSO, ISSM, SISSM, and SDSO are discussed. In addition, users may perform exercises at the end of each module to test their comprehension. A glossary of terms and points of contact within the INFOSEC community are provided for reference. The second volume includes workstation, network, and storage media security, as well as encryption, malicious activity, risk management, and auditing. Topics covered include workstation and operating systems basics, network basics (including vulnerabilities, examples of violations, and security services/devices), and types/ handling of storage media security .

Encryption, malicious code (including the spread and detection/prevention of malicious code, with an emphasis on viruses), fundamentals of risk management, and auditing goals are discussed. In addition, users may perform exercises at the end of each module to test their comprehension. The CD-ROM can be linked to your website for testing purposes. A glossary of terms and points of contact within the INFOSEC community are provide for reference. This product is based upon the NSA course ND225, Operational Information Systems Security. As we become more dependent upon our information systems, the vulnerability of these systems and **networks** grows. Incidents involving penetrating **computer networks** to obtain, corrupt, or destroy data are also on the rise. Because of this vulnerability, the Department of Defense (DOD) has developed this and other interactive CD-ROMs that provide awareness to this problem. While these products were developed for DOD employees, the information provided is applicable to anyone concerned with **computer security**.

15/7/11 (Item 3 from file: 8)

DIALOG(R) File 8: Ei Compendex(R)

(c) 2001 Engineering Info. Inc. All rts. reserv.

05012171 E.I. No: EIP98054193942

Title: Distributed events in active database systems: letting the genie out of the bottle

Author: Koschel, A.; Lockemann, P.C.

Corporate Source: Universitat Karlsruhe, Karlsruhe, Ger

Source: Data & Knowledge Engineering v 25 n 1-2 Mar 1998. p 11-28

Publication Year: 1998

CODEN: DKENEW **ISSN:** 0169-023X

Language: English

Document Type: JA; (Journal Article) **Treatment:** T; (Theoretical)

Journal Announcement: 9807W2

Abstract: Similar to grouping autonomous DBMSs within large-scale distributed, heterogeneous and loosely coupled **networks** into DBMS federations, active information sources may be grouped into active DBMS federations. The paper claims that as a prerequisite for such federations, **event handling** must be separated from the members of the federation and concentrated within an independent **network** component. Two consequences of such a decision are explored in the paper: The construction of suitable wrappers that perform the task of **event detection** for a large variety of active and passive information sources, and the unbundling of event processing based on ECA rules into a number of individual functions which can then be distributed across the **network** and configured into **event handlers** that pursue specific strategies. (Author abstract) 46 Refs.

15/7/12 (Item 4 from file: 8)

DIALOG(R) File 8: Ei Compendex(R)

(c) 2001 Engineering Info. Inc. All rts. reserv.

05005594 E.I. No: EIP98054178914

Title: Turning the lights back on in the data centre

Author: Noble, Charles

Corporate Source: Australian Water Technologies Pty Ltd, Aust

Conference Title: Proceedings of the 1997 23rd International Conference for the Resource Management & Performance Evaluation of Enterprise Computing Systems. Part 1 (of 2)

Conference Location: Orlando, FL, USA **Conference Date:** 19971207-19971212

E.I. Conference No.: 48275

Source: CMG Proceedings v 1 1997. CMG, Turnersville, NJ, USA. p 345-350

Publication Year: 1997

CODEN: CMPREY

Language: English

Document Type: CA; (Conference Article) **Treatment:** G; (General Review)

Journal Announcement: 9806W4

...System integrity must be addressed at all levels of hardware and software that comprise the **computer** system. Errors that occur could propagate to a regular storage media. WORM storage technology prevents these errors from corrupting data that has been properly **recorded** to an optical **WORM** disk. On the other hand, system security is the process and the physical barriers that...

...is permanent, secure, and invulnerable to accidental or intentional tampering. Moreover, WORM offers long-term **storage technique** that virtually eliminates accidental erasure of data. To understand just how stable the technology is, consider these description of today's most common **WORM recording** formats. One, ablative **WORM** uses a laser burn pits in the recording surface of an optical disk. Two, Continuous...

17/3, K/5 (Item 4 from file: 13)
DIALOG(R) File 13:BAMP
(c) 2001 Resp. DB Svcs. All rts. reserv.



01075118 01384618 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Control will cost you: Part 1 of 2 parts
(While it is possible to make enterprise systems-management problems simpler, it could be expensive in terms of time and budget)
Article Author(s): Gallagher, Sean
Information Week, p 56-58, 60+
February 23, 1998
DOCUMENT TYPE: Journal ISSN: 8750-6874 (United States)
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2740

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:

...SNMP

Automatic trap and
event handling

Supported by
NetView, Enterprise
Console, and
Distributed
Monitoring

tools are managing;
no integrated

network management

Supported through
ProVision **Event**
Management Common
Services; processes
internal and
external SNMP
alerts

Reduced management
bandwidth consumption
over **WAN** connections

Distributed
Monitoring,
Multiplexed
Distribution for
data from Tivoli
applications

Platinum Enterprise
Communicator
middleware

WAN and LAN
bandwidth-management
tools

Software
distribution
support for
bandwidth
throttling
through **WAN** -Smart
and parallel
distribution

Not available now

Network -management
into should be
stored in the common
data **repository**

Yes

Depends on
third-party tool

Alert and **event**
filtering capabilities
allow users to tune
level of information
to their needs

Tivoli Enterprise
Console, NetView,
Distributed
Monitoring proactive
management initiates

User-defined
thresholds and
alerts, **event**
filtering with
ProVision Event

| | predefined actions | Management; multiple alerts... |
|---|---|---|
| ...yet available user accounts and permissions across network operating systems | Administration handles user account configuration; support for single signon from third parties to come | (AutoSecure SSO ships end 1Q) |
| Delegation of... | | |
| ...interface and junior administrators | | |
| Multiple levels of access to network -management features | NetView Access | Third-party product, not integrated--none proposed |
| Audit network access, usage, and security, and integrate with security for access from outside the WAN and LAN | TME 10 Security Management, with Tivoli Access Control Facility | Third-party product, not integrated--none proposed |
| Integration of AS/400 management into network management | NetView for OS/390 | No integration |
| Integrate with asset management, and provide network -mapping capabilities | TME 10 Inventory Integration, NetView, and Enterprise Console | None yet |
| Distributed monitoring | TME 10 Distributed Monitoring | Platinum Data Exchange |
| Requirements | Bull | Computer Associates |
| Auto-discovery of IP, IPX, and SNA resources; IP resource management through SNMP | Supported by OpenMaster through ISM Discovery; administrator can specify networks explored | Supported by Unicenter TNG |
| Automatic trap and event handling | Supported by OpenMaster, ISM Alarm, and ISM Event Processor | Supported |
| Reduced management bandwidth consumption over WAN connections | OpenMaster, ISM Concentrator, and ISM Performance service | Distributed State Machine, message storm suppression |
| WAN and LAN bandwidth-management tools | Performance monitoring and statistics | Monitoring with Response Manager |
| Network -management into should be stored in the common data repository | Yes | Yes |
| Alert and event filtering capabilities allow users to tune level... | OpenMaster, ISM Alarm, and ISM Trouble Ticketing/ | Filtering , message storm suppression, notification by |
| ...management of user accounts and permissions across network operating | AccessMaster | Unicenter TNG Single signon interface for user security |

4/9/39 (Item 4 from file: 674)
DIALOG(R) File 674:Computer News Fulltext
(c) 2002 IDG Communications. All rts. reserv.

100846

VENDORS AIM TO HELP USERS SIMPLIFY NETWORK SECURITY.

VENDORS AIM TO HELP USERS SIMPLIFY NETWORK SECURITY.

Byline: BY TIM GREENE AND ELLEN MESSMER

Journal: Network World Page Number: 1

Publication Date: May 06, 2002

Word Count: 1160 Line Count: 110

Text:

LAS VEGAS - A slew of vendors this week will take the stage at NetWorld+Interop 2002 Las Vegas to highlight new products and services aimed at making networks safer. Vendors are looking to simplify this important task by processing multiple security applications on a single device, as is the case with start-up FortiNet. Others, such as Rainbow Technologies and Neoteris, will take advantage of ubiquitous Secure Sockets Layer technology to make Web access more secure and easier to set up. And still others, such as VeriSign, will offer services that let businesses turn over the burden of maintaining network integrity to someone else. For its part, FortiNet is introducing six models of its FortiGate security-processing gear that bundles firewall, VPN, virus scanning and other security functions. The platform is based on FortiNet security chips called FortiASIC, which scan for virus signatures, accelerate cryptography, process packets for firewall filtering and manage approved traffic flows. FortiGate can screen content by blocking all traffic from specified URLs and traffic from sites that are not banned but nevertheless contain banned content, the company says. A FortiGate box performs virus scanning at Agile Networks' headquarters in San Jose and supporting VPN connections to remote users, says Francis Leong, systems administrator for the software company. He had been using SonicWall gear, but wanted to get rid of license fees. He continues to use SonicWall appliances at remote sites for VPN links because they are already in place and interoperate with Fortinet's equipment. The FortiGate products, FG50, FG100, FG200, FG300, FG 400 and FG2000, range in price from about \$700 to \$40,000 and are available now for use in small-office to ISP data centers. To the world of SSL remote access, Rainbow is introducing NetSwift iGate, a secure Web-access device. NetSwift iGate sits behind a corporate firewall and establishes SSL sessions over the Internet with remote users, authenticates them and sets up communication between remote machines and Web-enabled applications on servers that are protected by the firewall. Rainbow also makes authentication hardware tokens that it packages with iGate so users can practice what's known as "two-factor authentication" rather than supplying just a username and password to access protected resources. NetSwift iGate costs \$10,000 for 50 users and \$90,000 for 3,000 users. It is scheduled to ship at the end of next month. One of iGate's competitors, Neoteris, is introducing a smaller-capacity version of its Employee Access proxy box. Employee Access 150 is meant for 100 to 150 users as opposed to the original, which supports 1,000. The smaller capacity comes with a lower price - \$10,000 vs. \$15,000 for the larger version - so it is more affordable for smaller businesses, the company says. Neoteris also is introducing support for authenticating users via external Lightweight Directory Access Protocol directories. Meanwhile, VeriSign will tout a new slew of managed security services for **intrusion** detection, VPNs and firewall monitoring to be provided through two operations centers, including its Herndon, Va., facility, where until now it only provided digital certificate and Domain Name services. A second VeriSign operations site will be at Downers Grove, Ill., the location of the managed security

services provider (MSSP) Telenesus it acquired last year. According to Bob McCullen, senior director for VeriSign managed security services, the range of equipment that VeriSign will remotely monitor on the customer's behalf includes the Cisco, Internet Security Systems and Enterasys Networks intrusion-detection systems (IDS), the Nokia and Check Point Software firewall/VPNs, and managed authentication services based on ActivCard hardware tokens. The company also will undertake managed virus scanning and content inspection. The fees will range from about \$2,000 to \$2,200 per month for IDS management, while managed authentication would range from \$3.50 to \$12 per user, per month. Managed firewall service would cost between \$1,000 and \$2,500 per month. All the services include help desk, reporting and event correlation, McCullen says. Of critical importance, VeriSign will rely on another MSSP, **Counterpane**, to help collect data from the customer's site and analyze it using **Counterpane**'s Sentry monitoring equipment. VeriSign will send customer data collected by Sentry to **Counterpane**'s security operations centers, where **Counterpane**'s Socrates analysis engine will analyze it to assess security threats. One Teleneus customer, National Tech Team, a help-desk outsourcing firm with \$100 million in annual revenues and 1,300 employees, says it was unaware of this arrangement, but expected to transition to being a regular VeriSign customer. "We need this type of service," says Maj Homa youn fal, National Tech Team's vice president of technology. "After Sept. 11, we wanted to be able to monitor day and night using IDS, and Teleneus had the know-how. And it's cost-effective." **Intrusion** detection at N+I For those interested in protecting their network devices from attack, Tripwire will have on exhibit Tripwire for Network Devices 2.0, the product evolution of what was formerly Tripwire for Routers and Switches. Introduced last fall, the server-based software for Solaris or Windows is used to lock down remotely made changes to Cisco IOS-based routers and switches. The Tripwire software also can restore files automatically if they are tampered with or destroyed in events such as power outages. Tripwire for Network Devices 2.0, which costs \$249 per node, extends data-integrity protection to Cisco's Catalyst switch, the Cisco PIX firewall and other vendor equipment, including the Hewlett-Packard ProCurve Switch and Foundry Networks and Extreme Networks gear. Tripwire also makes a product for server-data integrity, and Tripwire is showcasing Tripwire for Servers 3.0, which adds a way to report to the Check Point management console and the Tripwire for Manager 3.0 console, which costs around \$7,000. Also new is a separate Tripwire for the Check Point firewall so managers can be informed of changes to the Check Point firewall, both authorized and unauthorized. Costing about \$700, it will detect and report changes but not restore data. Trapping hackers Also at N+I, IDS vendor Recourse Technologies will unveil the third version of its ManTrap honeypot, a decoy computer used to spot hackers. ManTrap 3.0 adds a way to do "live-session playback" that can show an attack taking place graphically on the ManTrap console as it's occurring in near real time. ManTrap starts at \$7,500. In addition, says Fred Kost, senior vice president of marketing, Recourse will showcase ManHunt 2.1, which will be able to inspect traffic at 2G bit/sec, doubling the previous speed. Kost says a lot of the advance is possible because Intel processors are improving to help with processing power. ManHunt 2.1, which costs \$25,000, also will be able to use SQL to export data into reporting packages. Recourse which today will announce \$11 million in funding from Mesirow Financial, now has about 120 customers. Some customers say they also use ManTrap to look inside the corporate intranet for suspicious activity. "It can help in spotting someone trying to hack into your wireless LAN," says Jeff Uslan, director of information protection and security at Sony Pictures Entertainment. "Someone can be in a parking lot trying to do this."n

SECURITY WATCH: Your best defense against hack attacks: Good information and an insurance policy. (Company Business and Marketing)

McClure, Stuart; Scambray, Joel

InfoWorld, 22, 20, 52

May 15, 2000

ISSN: 0199-6649

LANGUAGE: English

RECORD TYPE: Fulltext

WORD COUNT: 690

LINE COUNT: 00060

TEXT:

IF YOU SPEND much time bantering in security circles, you're bound to hear the dogma: Technology won't solve your security problems anytime soon, so stick to the basics, such as policy, risk mitigation, vigilant monitoring, disaster preparedness, and -- most important -- keeping informed on the latest attack information. As disheartening as it may be, it is true.

So why are there still so many information-security-clueless companies, vendors, and end-users? Is it because security is so difficult? We don't think so. Rather, it's because definitive information on what the underground is doing to breach security is still kept rather hush-hush. The reasons range from victims trying to keep a low public relations profile on potentially embarrassing lapses to vendors trying to keep a competitive edge in an ever-expanding security product and services market. Whatever the reasons, they lack any hearty justification.

How to break this vicious circle of silence? In the past we've pushed for a public database of attack information. Security practitioners could anonymously contribute valuable information about security attacks; it could be supported by a minimal subscription. Would it work?

Many vendors have attempted to collect such data in various forms. For example, Internet Security Systems has demonstrated good citizenship by publishing its X-Force database of vulnerabilities over the years. A new initiative is underfoot called Common Vulnerabilities and Exposures (CVE), at www.cve.mitre.org, that is attempting to bring order to the madness that ravages the Internet every day.

We also enjoy reading many of the full-disclosure-oriented mailing lists such as those at securityfocus.com, sans.org, and ntsecurity.net. Two recent examples: Securityfocus' Incidents list recounts the "I Love You" worm's inner workings, and a highly interesting post appears on ntsecurity.net's Win2KsecAdvice list about a Windows NT and Windows 2000 Registry setting called MaxClientRequestBuffer.

One of the most frequently cited annual surveys on information security breaches is sponsored by the Computer Security Institute (CSI), at www.gocsi.com. The CSI essentially polls 500 security personnel and acts as a weather vane, but count us among those who yearn for more granular tracking of what's going on.

Another potential source of information is the new crop of managed monitoring services. For example, way back in the spring of 1998, we wrote a Test Center Comparison of **intrusion**-detection products. That article included IBM's Emergency Response Service (ERS), one component of which was the installation of Wheel Group's (now Cisco's) NetRanger network monitoring device on client sites and remote collection of attack data. At the time, an IBM employee intimated that the company was building an interesting meta data set of attack information from dozens of clients around the world. We wonder what ever became of this database. Is IBM going to publish this pot of gold?

Cryptography guru Bruce Schneier recently put his company, **Counterpane** (www.counterpane.com), behind a Managed Security Monitoring service, which will collect security data to be parsed by software filters, and even human expertise, in **Counterpane**'s data centers.

We talked recently with Schneier, and he sounded confident that Counterpane would make its data publicly available, at least to the extent that it isn't injurious to client confidentiality concerns. "As far as I know, there isn't any real data on the incidence or frequency or type of attacks in the real world," Schneier said. "This will be a very valuable research result." If no one will listen to us, maybe Schneier can get them to take notice.

Is your organization regularly reviewing firewall logs and tracking potential threats, trying to understand what'll happen next? If you're anything like the companies we see day in and day out, the answer is no. It's about time we let someone else do it for us. Contribute to our database of e-mail attacks at security_watch@infoworld.com.

Stuart McClure is president/CTO and Joel Scambray is a managing principal at security consultant Foundstone (www.foundstone.com), formerly Rampart Security Group.

Copyright (c) 2000 InfoWorld Media Group Inc
COPYRIGHT 2000 InfoWorld Publishing Co.

COMPANY NAMES: Internet Security Systems--Services
GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Company services; Database industry
EVENT CODES/NAMES: 360 Services information
PRODUCT/INDUSTRY NAMES: 7375000 (Database Providers)
SIC CODES: 7375 Information retrieval services
NAICS CODES: 514191 On-Line Information Services
FILE SEGMENT: CD File 275